

Introduced by Senator Simitian

February 20, 2007

An act to repeal and amend Section 1798.29 of the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

SB 364, as introduced, Simitian. Personal information: privacy.

Existing law requires any agency that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Existing law allows an agency to provide that disclosure by substitute notice, as specified, if the agency demonstrates that the cost of disclosure would exceed \$250,000, or that the affected class exceeds 500,000 persons, or that the agency does not have sufficient contact information.

In addition to the other substitute notice provisions, this bill would instead allow for substitute notice if the agency demonstrates that the cost of disclosure would exceed \$100,000. The bill would also repeal a duplicative provision of law.

Vote: majority. Appropriation: no. Fiscal committee: no.
State-mandated local program: no.

The people of the State of California do enact as follows:

- 1 SECTION 1. Section 1798.29 of the Civil Code, as added by
- 2 Section 2 of Chapter 915 of the Statutes of 2002, is repealed.

1 ~~1798.29.— (a) Any agency that owns or licenses computerized~~
2 ~~data that includes personal information shall disclose any breach~~
3 ~~of the security of the system following discovery or notification~~
4 ~~of the breach in the security of the data to any resident of California~~
5 ~~whose unencrypted personal information was, or is reasonably~~
6 ~~believed to have been, acquired by an unauthorized person. The~~
7 ~~disclosure shall be made in the most expedient time possible and~~
8 ~~without unreasonable delay, consistent with the legitimate needs~~
9 ~~of law enforcement, as provided in subdivision (c), or any measures~~
10 ~~necessary to determine the scope of the breach and restore the~~
11 ~~reasonable integrity of the data system.~~

12 ~~(b) Any agency that maintains computerized data that includes~~
13 ~~personal information that the agency does not own shall notify the~~
14 ~~owner or licensee of the information of any breach of the security~~
15 ~~of the data immediately following discovery, if the personal~~
16 ~~information was, or is reasonably believed to have been, acquired~~
17 ~~by an unauthorized person.~~

18 ~~(c) The notification required by this section may be delayed if~~
19 ~~a law enforcement agency determines that the notification will~~
20 ~~impede a criminal investigation. The notification required by this~~
21 ~~section shall be made after the law enforcement agency determines~~
22 ~~that it will not compromise the investigation.~~

23 ~~(d) For purposes of this section, “breach of the security of the~~
24 ~~system” means unauthorized acquisition of computerized data that~~
25 ~~compromises the security, confidentiality, or integrity of personal~~
26 ~~information maintained by the agency. Good faith acquisition of~~
27 ~~personal information by an employee or agent of the agency for~~
28 ~~the purposes of the agency is not a breach of the security of the~~
29 ~~system, provided that the personal information is not used or~~
30 ~~subject to further unauthorized disclosure.~~

31 ~~(e) For purposes of this section, “personal information” means~~
32 ~~an individual’s first name or first initial and last name in~~
33 ~~combination with any one or more of the following data elements,~~
34 ~~when either the name or the data elements are not encrypted:~~

35 ~~(1) Social security number.~~

36 ~~(2) Driver’s license number or California Identification Card~~
37 ~~number.~~

38 ~~(3) Account number, credit or debit card number, in combination~~
39 ~~with any required security code, access code, or password that~~
40 ~~would permit access to an individual’s financial account.~~

1 ~~(f) For purposes of this section, “personal information” does~~
2 ~~not include publicly available information that is lawfully made~~
3 ~~available to the general public from federal, state, or local~~
4 ~~government records.~~

5 ~~(g) For purposes of this section, “notice” may be provided by~~
6 ~~one of the following methods:~~

7 ~~(1) Written notice.~~

8 ~~(2) Electronic notice, if the notice provided is consistent with~~
9 ~~the provisions regarding electronic records and signatures set forth~~
10 ~~in Section 7001 of Title 15 of the United States Code.~~

11 ~~(3) Substitute notice, if the agency demonstrates that the cost~~
12 ~~of providing notice would exceed two hundred fifty thousand~~
13 ~~dollars (\$250,000), or that the affected class of subject persons to~~
14 ~~be notified exceeds 500,000, or the agency does not have sufficient~~
15 ~~contact information. Substitute notice shall consist of all of the~~
16 ~~following:~~

17 ~~(A) E-mail notice when the agency has an e-mail address for~~
18 ~~the subject persons.~~

19 ~~(B) Conspicuous posting of the notice on the agency’s Web site~~
20 ~~page, if the agency maintains one.~~

21 ~~(C) Notification to major statewide media.~~

22 ~~(h) Notwithstanding subdivision (g), an agency that maintains~~
23 ~~its own notification procedures as part of an information security~~
24 ~~policy for the treatment of personal information and is otherwise~~
25 ~~consistent with the timing requirements of this part shall be deemed~~
26 ~~to be in compliance with the notification requirements of this~~
27 ~~section if it notifies subject persons in accordance with its policies~~
28 ~~in the event of a breach of security of the system.~~

29 SEC. 2. Section 1798.29 of the Civil Code, as added by Section
30 2 of Chapter 1054 of the Statutes of 2002, is amended to read:

31 1798.29. (a) Any agency that owns or licenses computerized
32 data that includes personal information shall disclose any breach
33 of the security of the system following discovery or notification
34 of the breach in the security of the data to any resident of California
35 whose unencrypted personal information was, or is reasonably
36 believed to have been, acquired by an unauthorized person. The
37 disclosure shall be made in the most expedient time possible and
38 without unreasonable delay, consistent with the legitimate needs
39 of law enforcement, as provided in subdivision (c), or any measures

1 necessary to determine the scope of the breach and restore the
2 reasonable integrity of the data system.

3 (b) Any agency that maintains computerized data that includes
4 personal information that the agency does not own shall notify the
5 owner or licensee of the information of any breach of the security
6 of the data immediately following discovery, if the personal
7 information was, or is reasonably believed to have been, acquired
8 by an unauthorized person.

9 (c) The notification required by this section may be delayed if
10 a law enforcement agency determines that the notification will
11 impede a criminal investigation. The notification required by this
12 section shall be made after the law enforcement agency determines
13 that it will not compromise the investigation.

14 (d) For purposes of this section, “breach of the security of the
15 system” means unauthorized acquisition of computerized data that
16 compromises the security, confidentiality, or integrity of personal
17 information maintained by the agency. Good faith acquisition of
18 personal information by an employee or agent of the agency for
19 the purposes of the agency is not a breach of the security of the
20 system, provided that the personal information is not used or
21 subject to further unauthorized disclosure.

22 (e) For purposes of this section, “personal information” means
23 an individual’s first name or first initial and last name in
24 combination with any one or more of the following data elements,
25 when either the name or the data elements are not encrypted:

26 (1) Social security number.

27 (2) Driver’s license number or California Identification Card
28 number.

29 (3) Account number, credit or debit card number, in combination
30 with any required security code, access code, or password that
31 would permit access to an individual’s financial account.

32 (f) For purposes of this section, “personal information” does
33 not include publicly available information that is lawfully made
34 available to the general public from federal, state, or local
35 government records.

36 (g) For purposes of this section, “notice” may be provided by
37 one of the following methods:

38 (1) Written notice.

1 (2) Electronic notice, if the notice provided is consistent with
2 the provisions regarding electronic records and signatures set forth
3 in Section 7001 of Title 15 of the United States Code.

4 (3) Substitute notice, if the agency demonstrates that the cost
5 of providing notice would exceed ~~two~~ *one* hundred ~~fifty~~ thousand
6 dollars ~~(\$250,000)~~ *(\$100,000)*, or that the affected class of subject
7 persons to be notified exceeds 500,000, or the agency does not
8 have sufficient contact information. Substitute notice shall consist
9 of all of the following:

10 (A) E-mail notice when the agency has an e-mail address for
11 the subject persons.

12 (B) Conspicuous posting of the notice on the agency's Web site
13 page, if the agency maintains one.

14 (C) Notification to major statewide media.

15 (h) Notwithstanding subdivision (g), an agency that maintains
16 its own notification procedures as part of an information security
17 policy for the treatment of personal information and is otherwise
18 consistent with the timing requirements of this part shall be deemed
19 to be in compliance with the notification requirements of this
20 section if it notifies subject persons in accordance with its policies
21 in the event of a breach of security of the system.